

P A T E N T C L A I M S

1. Network security system for detecting security relevant irregularities in a network, comprising
data sources located on and/ or constituting the network, with
means for generating network-security relevant data;
an input module, with
input handlers for various protocols to connect to the data sources;
at least one processing module, connected to said input module for access to said data sources, with
means for translating said network-security relevant data into quantitative variables;
a supervisory system, with
means for presenting processed data to a security system operator; and
an interface module, with
means for transferring said quantitative variables from the processing module to the supervisory system.
2. Security system as in claim 1, characterized in, that
said data sources comprise routers, firewalls, hosts, applications, switches, NIDS, HIDS or any combination thereof.
3. Security system as in any of claims 1 or 2, characterized in, that
the network-security relevant data consists of
numerical values maintained via increment/decrement operations, rate calculations, pass-through of values or evaluation of mathematical expressions involving multiple values or any combination thereof, and /or
textual values maintained via template matching, text transformation, text translation, and composition of text from templates, text strings from incoming data and numerical values from incoming data or any combination thereof.

4. Security system as in any of claims 1 or 3, characterized in, that
said supervisory system comprises
means for displaying said variables to an system operator, and
reaction facilities with means for initiating predefined countermeasures.
5. Security system as in any of claims 1 to 4, characterized in, that
the processing modules act on individual incoming data messages and batches of
those messages.
6. Security system as in any of claims 1 to 5, characterized in, that
the displaying means display the security status/health information as quantitative trend
graphs with historical data storage and zoom in/out function.
7. Security system as in any of claims 1 to 6, characterized in, that
the displaying means display a schematical depiction of the network and device
structure and topology.
8. Security system as in claims 7, characterized in, that
the visual elements denote security status by means of coloring and/or numerical
and/or textual annotations
9. Security system as in any of claims 1 to 8, characterized in, that
the system further comprises
storage means for maintaining temporary and persistent records of the results of
the processing steps for later in-depth analysis.
10. Automation system operator workstation in a network with an automation system,
comprising
means for controlling the processes of the automation system over the network, said
controlling means comprising a human machine interface with means for displaying
information about the automation system to an automation system operator and means
for entering commands for controlling the automation system,
said automation system operator workstation being connected to a security system as
claimed in any of the preceding claims, wherein
the supervisory system is integrated into the automation system controlling means,

said status and trend presenting means being included in the information displaying system of the human machine interface, and said countermeasures initiating means being integrated in the commands entering means.